ViPNet SafePoint

Модели администрирования и синхронизации настроек

infotecs

ФРКЕ.00240-01 32 04

Версия продукта 1.0.0

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Аннотация

В данном документе рассматриваются модели администрирования и синхронизации настроек в системе защиты информации ViPNet SafePoint для ОС Microsoft Windows (далее СЗИ ViPNet SafePoint). В документе не приводятся описание действий администратора по работе с сервером безопасности СЗИ ViPNet SafePoint или интерфейсом управления настройками клиентской части СЗИ ViPNet SafePoint, описание действий приводится в документах «ViPNet SafePoint. Руководство администратора по локальному администрированию» и «ViPNet SafePoint. Руководство администратора по удаленному администрированию».

Оглавление

1. Средства администрирования СЗИ ViPNet SafePoint. Задачи синхронизации настроек

К средствам администрирования в СЗИ ViPNet SafePoint относятся:

- локальный интерфейс настройки клиентской части;
- сервер безопасности – отдельный компонент, решающий задачи удаленного администрирования клиентских частей, удаленной работы с журналами аудита событий безопасности в интерактивном режиме, удаленного управления защищаемыми компьютерами, на которые установлены клиентские части. Серверы безопасности могут образовывать иерархию удаленного администрирования. Функция удаленного управления защищаемыми компьютерами может быть отключена при установке сервера;
- сервер аудита – отдельный компонент, решающий задачи удаленной работы с журналами аудита событий безопасности в интерактивном режиме и в реальном времени, удаленного управления защищаемыми компьютерами, на которые установлены клиентские части (в случае установки сервера безопасности и сервера аудита на одном компьютере).

Настройка клиентской части СЗИ ViPNet SafePoint может осуществляться как локально, так и удалено – с сервера безопасности.

К архитектурным особенностям СЗИ ViPNet SafePoint может быть отнесено:

- одна и та же клиентская часть может подключаться к неограниченному числу серверов безопасности, с каждого из которых может осуществляться ее настройка, и к неограниченному числу серверов аудита;
- серверы безопасности могут относиться к ведомым и ведущим для реализации моделей иерархического администрирования;
- серверы безопасности и серверы аудита могут устанавливаться как на один, так и на различные компьютеры – функционально эти задачи разделены;
- для защиты компьютеров с установленными на них серверами безопасности и/или серверами аудита, на эти компьютеры также должны устанавливаться клиентские части, которые могут настраиваться, как из локального интерфейса, так и из интерфейсов серверов безопасности, включая сервер безопасности, установленный на один компьютер с клиентской частью.

Т.к. одна и та же часть клиентская часть может подключаться к неограниченному числу серверов безопасности и серверов аудита, предоставляется возможность решения различных задач при использовании в одной сети одновременно нескольких соответствующих серверов:

- задача резервирования серверов безопасности (могут резервироваться серверы безопасности обоих уровней иерархии – и ведомые, и ведущие);
- задача разделения нагрузки на серверы безопасности (может разделяться нагрузка между серверами безопасности обоих уровней иерархии – и между ведомыми, и между ведущими);
- задача ограниченного администрирования (без возможности удаленного управления защищаемыми компьютерами) клиентскими частями СЗИ ViPNet SafePoint, установленными на компьютеры, к обрабатываемой информации на которых доступ администратора безопасности должен ограничиваться;
- задача функционального разделения задач удаленного администрирования и аудита на различных рабочих местах (компьютерах) администраторов безопасности.

Поскольку в общем случае в сетевой системе защиты информации существуют различные возможности (средства) настройки клиентских частей, решается задача их синхронизации, в части:

- предоставления возможности настройки клиентской части СЗИ ViPNet SafePoint в любой момент времени только из одного интерфейса (либо локального, либо удаленного) – синхронизация процесса осуществления настройки клиентских частей;
- автоматической (либо автоматизированной) синхронизации настроек клиентской части СЗИ ViPNet SafePoint на всех средствах, из интерфейсов которых они могут быть заданы/изменены, на которых хранятся данные настройки, что обеспечивает единство в любой момент времени настроек любой клиентской части в сетевой системе защиты информации.

Т.к. несколько серверов безопасности, интерфейсы которых могут использоваться для настроек одной клиентской части СЗИ ViPNet SafePoint, могут образовывать, как один, так и различные уровни иерархии удаленного администрирования, синхронизация настроек клиентских частей СЗИ ViPNet SafePoint реализуется между серверами безопасности, как одного, так и различных уровней иерархии администрирования. Для серверов безопасности различных уровней иерархии администрирования возможны различные режимы синхронизации, определяемыми различными режимами контроля действий ведомым ведущим сервером безопасности.

Поскольку задача удаленного администрирования с сервера безопасности любого уровня иерархии направлена, в конечном счете, на задание/изменение настроек именно клиентских частей (ключевым моментом реализации защиты является не то, какие настройки заданы на той или иной серверной части, а то, какие, настройки действуют на клиентской части, реализующей защиту информации) синхронизирующим элементом в сетевой системе защиты информации является именно клиентская часть СЗИ ViPNet SafePoint, настройки серверов безопасности синхронизируются через настройки клиентских частей. Как следствие, архитектурной особенностью сетевой системы защиты является не соединение серверов (как одного, так и различных уровней иерархии) между собою, а их соединение только с клиентскими частями

(между собою напрямую серверы безопасности не соединяются). При этом с ведущих серверов безопасности удаленно могут осуществляться настройки клиентских частей (в полном объеме могут администрировать клиентские части), устанавливаемых на компьютеры, на которых установлены ведомые серверы безопасности.

2. Базовые модели администрирования и синхронизации настроек

2.1. Модель синхронизации процесса настройки клиентских частей

Настройка механизмов защиты СЗИ ViPNet SafePoint может производиться как с использованием локального интерфейса управления настройками (клиентская часть СЗИ ViPNet SafePoint), так и с сервера безопасности СЗИ ViPNet SafePoint, путем запуска интерфейса управления настройками удаленно. При этом настройка одновременно может производиться только с использованием одного интерфейса управления настройками, вне зависимости от числа серверов (и их иерархии), к которым подключена эта клиентская часть.

При запущенном интерфейсе клиентской части СЗИ ViPNet SafePoint локально или с сервера безопасности, на ином сервере безопасности данная клиентская часть будет отображаться пиктограммой  , интерфейс ее настройки не сможет быть запущен на этом севере безопасности.

Если же интерфейс управления настройками СЗИ ViPNet SafePoint был запущен с сервера безопасности, то при попытке его запуска локально, на защищаемом компьютере будет выведено сообщение о невозможности запуска локального интерфейса настройки клиентской части (см. рис. 1).

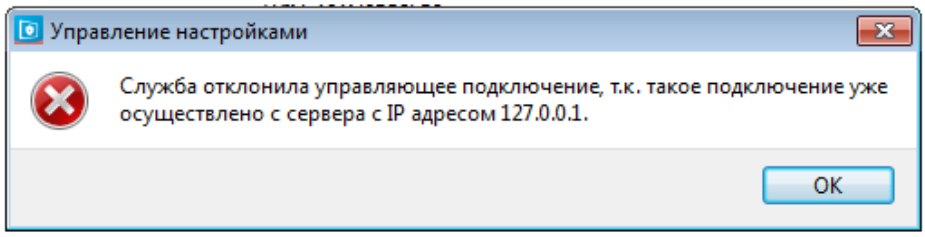

Рис. 1. Сообщение об отклонении запроса запуска локального интерфейса настройки клиентской части

2.2. Модели администрирования автономных клиентских частей

Рассматриваемая модель администрирования подразумевает, что на защищаемых объектах установлены автономные клиентские части СЗИ «ViPNet SafePoint» - сервер безопасности не используется, настройка возможна только из локального интерфейса. В данном случае, возможны следующие конфигурации:

1. Защищаемый объект входит в состав одноранговой сети. В этом случае вся настройка механизмов защиты информации происходит локально с использованием локального интерфейса управления настройками.

2. Защищаемый объект входит в состав доменной сети. В этом случае вся настройка механизмов защиты информации также происходит локально с использованием локального интерфейса управления настройками. Отличие решения задачи администрирования при данной конфигурации состоит в том, что администратору защищаемого компьютера предоставляется возможность создания/редактирования не только локальных, но и доменных пользователей. Для реализации данной возможности, при установке клиентской части СЗИ ViPNet SafePoint необходимо провести дополнительное конфигурирование устанавливаемой клиентской части. Действия необходимые для этого описаны в разделе 3.2 данного документа. При этом администратору безопасности защищаемого компьютера необходимо иметь права администратора домена.

2.3. Модели сетевого администрирования и синхронизации настроек с одним сервером безопасности СЗИ ViPNet SafePoint

Данная модель подразумевает наличие некоторого числа защищаемых компьютеров, с установленными на них клиентскими частями СЗИ ViPNet SafePoint, которые подключены к одному серверу безопасности СЗИ ViPNet SafePoint (см. рис. 2).

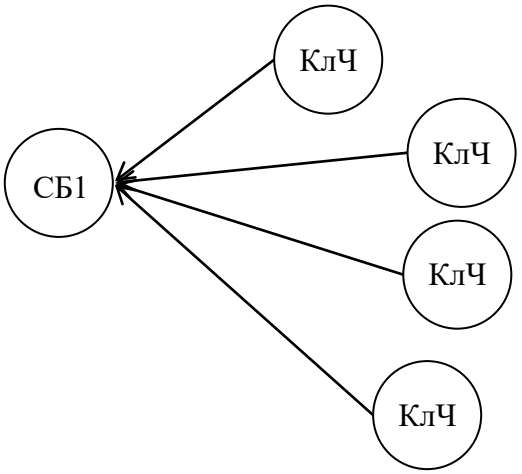

Рис. 2. Модель администрирования с одним сервером безопасности

Сервер безопасности СЗИ ViPNet SafePoint может быть установлен как на выделенный компьютер одновременно с клиентской частью СЗИ ViPNet SafePoint (для его защиты), при этом данная клиентская часть может быть, как подключена к серверу безопасности, в этом случае процесс ее администрирования аналогичен процессу администрирования других клиентских частей (установленных на удаленных компьютерах), так и не подключена. В последнем случае администрирование определяется моделью, описанной в разделе 2.2 данного документа.

Сервер безопасности СЗИ ViPNet SafePoint служит для удаленного администрирования клиентских частей СЗИ ViPNet SafePoint. Для защиты компьютера, с установленным севером безопасности СЗИ ViPNet SafePoint, необходима установка на данную машину клиентской части СЗИ ViPNet SafePoint.

Возможны следующие конфигурации:

1. Сервер безопасности и клиентская часть СЗИ ViPNet SafePoint установлены на компьютерах, входящих в состав одноранговой сети.

2. Сервер безопасности и клиентская часть СЗИ ViPNet SafePoint установлены на компьютерах, входящих в состав доменной сети. В данном случае следует назначить сервер безопасности главным по пользователям домена(установлен 1-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config), при этом редактирование базы данных пользователей домена будет возможно с компьютера, на котором установлен сервер безопасности, с использованием специальной утилиты, далее база данных доменных пользователей будет автоматически рассылаться на все подключенные к данному серверу безопасности клиентские части СЗИ ViPNet SafePoint. Администратор на сервере безопасности должен иметь права администратора домена.

В обоих случаях настройка механизмов защиты может происходить как локально, так и удаленно, при этом для удобства администрирования и исключения возможных конфликтов на сервере безопасности могут быть настроены автоматические действия, т.е. реакции на определенные события, произошедшие с настройками механизмов защиты на защищаемом объекте, с целью их синхронизации. Автоматические действия могут быть заданы исходя из следующих вариантов (режимов работы):

1. **Настройка** всех механизмов защиты клиентской части происходит **только с сервера безопасности** СЗИ ViPNet SafePoint (за исключением первичной настройки). В этом случае, если произошли какие-либо изменения настроек клиентской части, не вызванные действиями администратора с сервера безопасности СЗИ ViPNet SafePoint, на клиентскую часть автоматически будет отправлен эталонный (хранящийся на сервере безопасности) набор файлов настроек.

2. **Настройка** механизмов защиты клиентской части происходит как **с сервера безопасности** СЗИ ViPNet SafePoint, так **и локально** с использованием интерфейса клиентской части СЗИ ViPNet SafePoint. В данном случае, администратор может проводить настройку механизмов защиты локально и удаленно, при локальной настройки сервер безопасности будет автоматически принимать эти настройки (измененные администратором с использованием

интерфейса клиентской части СЗИ ViPNet SafePoint), при удаленной настройке клиентская часть будет автоматически принимать эти настройки.

3. **Настройка** всех механизмов защиты происходит **под контролем администратора сервера безопасности** СЗИ ViPNet SafePoint. В данном варианте не настраиваются автоматические реакции на события локального изменения настроек клиентской части СЗИ ViPNet SafePoint. При изменении настроек СЗИ ViPNet SafePoint с использованием локального интерфейса на сервере безопасности администратору будет предоставлен выбор действий:

- Отправить (восстановить) настройки. В этом случае на клиентскую часть будут отправлены настройки, хранящиеся на сервере.
- Принять настройки. В этом случае на серверную часть будут отправлены настройки, настроенные на клиентской части.
- Игнорировать. При выборе данного действия настройки не будут синхронизированы. При следующем подключении клиентской части к серверу безопасности, администратору вновь будет предложен выбор действий по синхронизации настроек. Кроме того, администратор может принудительно в любой момент времени получить или отправить настройки на клиентскую часть СЗИ ViPNet SafePoint. При этом до отправки настроек с сервера безопасности, на клиентской части будут действовать измененные локально настройки.

Режим контроля администратором сервера безопасности всех действий по изменению настроек клиентских частей может быть использован в любой конфигурации защищаемой сети.

2.4. Модели сетевого администрирования и синхронизации настроек с несколькими серверами безопасности СЗИ ViPNet SafePoint

Данная модель подразумевает наличие некоторого числа защищаемых объектов, с установленными клиентскими частями СЗИ ViPNet SafePoint, которые подключены к нескольким серверам безопасности СЗИ ViPNet SafePoint (см. рис. 3).

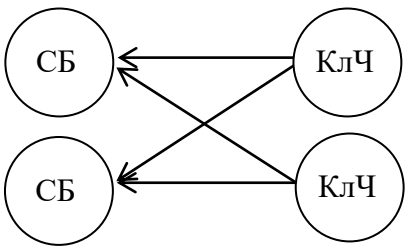

Рис. 3.Модель администрирования с несколькими серверами безопасности

Отличие данной модели администрирования от модели, рассмотренной в разделе 2.2, состоит в том, что необходима реализация соответствующего регламента администрирования клиентских частей с различных серверов безопасности СЗИ ViPNet SafePoint и регламента синхронизации настроек клиентских частей. Данный регламент задается назначением автоматических действий (реакций на определенные события) на серверах безопасности СЗИ ViPNet SafePoint.

2.4.1. Модели неиерархического администрирования

2.4.1.1. Регламенты администрирования и синхронизации настроек

При реализации моделей неиерархического администрирования, подразумевающих наличие в сетевой системе защиты нескольких равноправных серверов безопасности СЗИ ViPNet SafePoint, возможны следующие регламенты администрирования и синхронизации настроек:

1) Режим **«взаимного доверия»:**

- **настройка** клиентских частей СЗИ ViPNet SafePoint происходит **только с серверов безопасности**. В данном случае администраторы безопасности «доверяют» друг другу, т.е. автоматически на серверах безопасности принимаются настройки клиентских частей, внесенные другим сервером безопасности СЗИ ViPNet SafePoint, при этом автоматически происходит синхронизация настроек на всех серверах безопасности. Для реализации необходимо задать автоматические реакции получения настроек с серверов безопасности серверами безопасности. Поскольку настройка механизмов защиты происходит только удаленно, на события изменения настроек механизмов защиты с использованием локального интерфейса необходимо настроить автоматическое действие отправки набора настроек, хранящегося на сервере безопасности СЗИ ViPNet SafePoint, при этом измененные настройки на клиентской части с использованием локального интерфейса будут автоматически восстановлены с сервера безопасности;
- **настройка** клиентских частей СЗИ ViPNet SafePoint происходит как **с серверов безопасности**, так **и локально** на клиентских машинах, с использованием локального интерфейса клиентской части СЗИ ViPNet SafePoint. В данной конфигурации сервера безопасности принимают настройки клиентских частей, как внесенные другим сервером безопасности СЗИ ViPNet SafePoint, так и настройки, внесенные с использованием локального интерфейса.

2) Режим **«недоверия»**:

- **настройка** клиентских частей СЗИ «ViPNet SafePoint» происходит **только с серверов безопасности**. В данном случае на серверах безопасности не настраиваются автоматические действия, регламентирующие события изменения настроек, внесенных с других серверов безопасности СЗИ ViPNet SafePoint. При внесении изменений в настройки механизмов защиты клиентских частей с одного сервера безопасности, администратор другого сервера

безопасности может принять внесенные изменения (получить измененные файлы настроек), отправить хранящиеся у него файлы настроек – восстановить исходные настройки, или проигнорировать данное событие. Поскольку настройка механизмов защиты происходит только удаленно, на события изменения настроек механизмов защиты с использованием локального интерфейса необходимо настроить автоматическое действие отправки настроек, хранящихся на сервере безопасности СЗИ ViPNet SafePoint, при этом измененные настройки на клиентской части с использованием локального интерфейса будут автоматически восстановлены с сервера безопасности;

- **настройка** клиентских частей СЗИ ViPNet SafePoint происходит как **с серверов безопасности**, так **и локально** на клиентских машинах, с использованием локального интерфейса клиентской части СЗИ ViPNet SafePoint. В этом режиме автоматические действия на события изменения настроек механизмов защиты с использованием интерфейса изменения настрое СЗИ ViPNet SafePoint локально или удаленно не задаются, в результате этого при расхождении настроек на защищаемом объекте и хранящихся на сервере безопасности, администратор может принять измененные настройки (получить измененные файлы настроек), восстановить исходные настройки на клиентской части или проигнорировать данное событие.

3) **Режим «контроля»**. В данном режиме не задаются автоматические действия на события изменения настроек клиентских частей СЗИ ViPNet SafePoint, т.е. при изменении настроек клиентской части локально или с одного из серверов безопасности на серверах безопасности (кроме того, с которого были произведены изменения) администраторам будет предоставлена возможность просмотра и анализа внесенных изменений и дальнейший выбор действия – получить или отправить все настройки либо отдельные файлы настроек или игнорировать данные изменения.

Наличие нескольких серверов безопасности СЗИ ViPNet SafePoint позволяет реализовывать следующие режимы их использования в сетевой системе защиты информации:

1. Полное резервирование серверов безопасности.
2. Частичное резервирование серверов безопасности при наличии критичных по обрабатываемой информации объектов защиты.
3. Частичное резервирование серверов безопасности при наличии критичных к непрерывности контроля защищенности и администрирования объектов защиты.

2.4.1.2. Режимы использования серверов безопасности

2.4.1.2.1. Полное резервирование серверов безопасности

В данном режиме серверы безопасности обладают одинаковыми возможностями по администрированию клиентских частей и могут полностью заменить друг друга. В таком случае при выходе одно сервера безопасности из строя, либо по иным причинам, другой сервер безопасности может полностью его заменить.

Все клиентские части должны подключаться ко всем серверам безопасности. Схема взаимодействия серверов безопасности с клиентскими частями при полном резервировании серверов безопасности представлена на рис. 4.

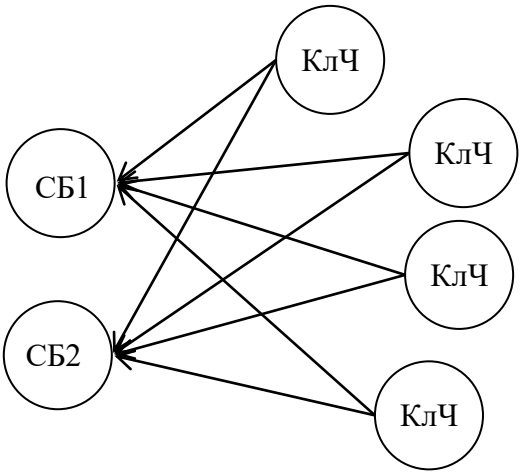

Рис. 4. Модель полного резервирования серверов безопасности

В случае доменной структуры функцию главного по доменным пользователям может выполнять любой (один) сервер безопасности.

2.4.1.2.2. Частичное резервирование серверов безопасности при наличии критичных объектов защиты

При реализации защиты информационной системы в случае, если в нее включены некоторые критичные к хищению информации защищаемые компьютеры (например, АРМ Генерального директора или Главного бухгалтера), с установленной клиентской частью СЗИ ViPNet SafePoint, возможность их администрирования может быть доверена только одному администратору – только с одного сервера безопасности.

Клиентские же части, установленные на остальные компьютеры, могут подключаться ко всем серверам безопасности, т.е. для них при этом реализовано полное резервирование серверов безопасности. Соответствующая схема администрирования представлена на рис. 5.

В случае доменной структуры функцию главного по доменным пользователям выполняет тот сервер безопасности, к которому подключены все клиентские части (на рис. 5 это сервер безопасности 1).

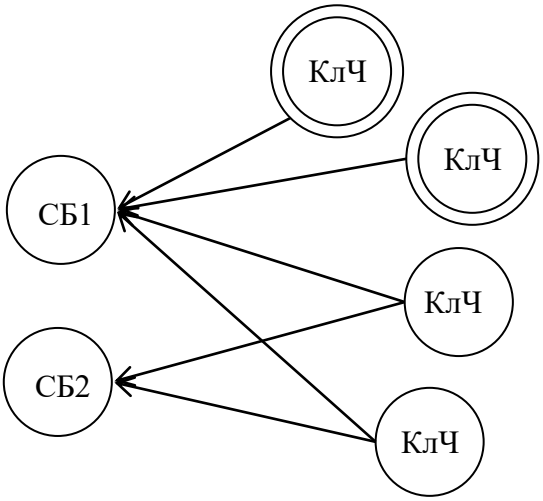

Рис. 5. Модель частичного резервирования серверов безопасности при наличии критичных по обрабатываемой информации объектов защиты

2.4.1.2.3. Частичное резервирование серверов безопасности при наличии критичных к непрерывности контроля защищенности и администрирования объектов защиты

При реализации защиты информационной системы в случае, если в нее включены некоторые крайне важные, критичные к непрерывности контроля защищенности и администрирования компьютеры, с установленной клиентской частью СЗИ ViPNet SafePoint, контроль которых необходим постоянно, то возможность их администрирования должна быть доверена одновременно со всех серверов безопасности (в отношении них реализуется полное резервирование). При этом можно разделить нагрузку между серверами безопасности в части настройки остальных клиентских частей.

Соответствующая схема администрирования представлена на рис. 6.

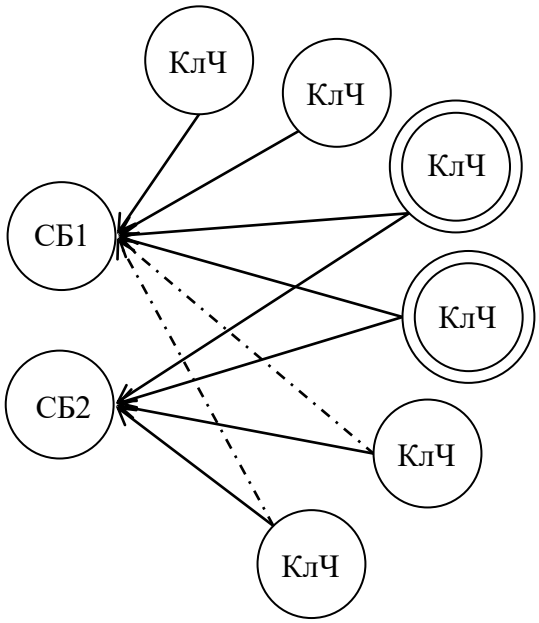

Рис. 6. Модель частичного резервирования серверов безопасности при наличии критичных к непрерывности контроля защищенности и администрирования объектов защиты

В случае доменной структуры функцию главного по доменным пользователям выполняет только один сервер безопасности, к которому должны подключаться все клиентские части (на рис. 6. - сервер безопасности 1).

При реализации подобных моделей в доменной сети только один сервер безопасности назначается главным по пользователям в домене, на других – настраивается реакция «получение настроек» на событие изменения базы данных доменных пользователей главным по пользователям домена сервером безопасности СЗИ ViPNet SafePoint.

2.4.2. Модели иерархического администрирования

Модели иерархического администрирования подразумевает наличие нескольких уровней иерархии серверов безопасности СЗИ ViPNet SafePoint (см. рис. 7). Сервер (серверы) безопасности СЗИ ViPNet SafePoint высшего уровня иерархии могут выполнять следующие функции:

- администрирование всех подключенных клиентских частей;
- контроль действий по администрированию клиентских частей серверами безопасности более низкого уровня иерархии;
- администрирование критически важных защищаемых объектов.

Иерархическое администрирование применимо как в одноранговой сети, так и в доменной сети. При использовании СЗИ ViPNet SafePoint в доменной структуре, на всех серверах безопасности всех уровней иерархии необходимо добавить автоматическое действие «Получить все настройки» в качестве реакции на событие «Обновлена база данных пользователей домена AD» (с указанием IP адреса или имени сервера безопасности, с которого осуществляется администрирование базы данных пользователей домена).

Для каждого уровня иерархии серверов может быть применена одна из моделей неиерархического администрирования с несколькими серверами безопасности, рассмотренных выше, с соответствующими для них режимами администрирования и синхронизации настроек.

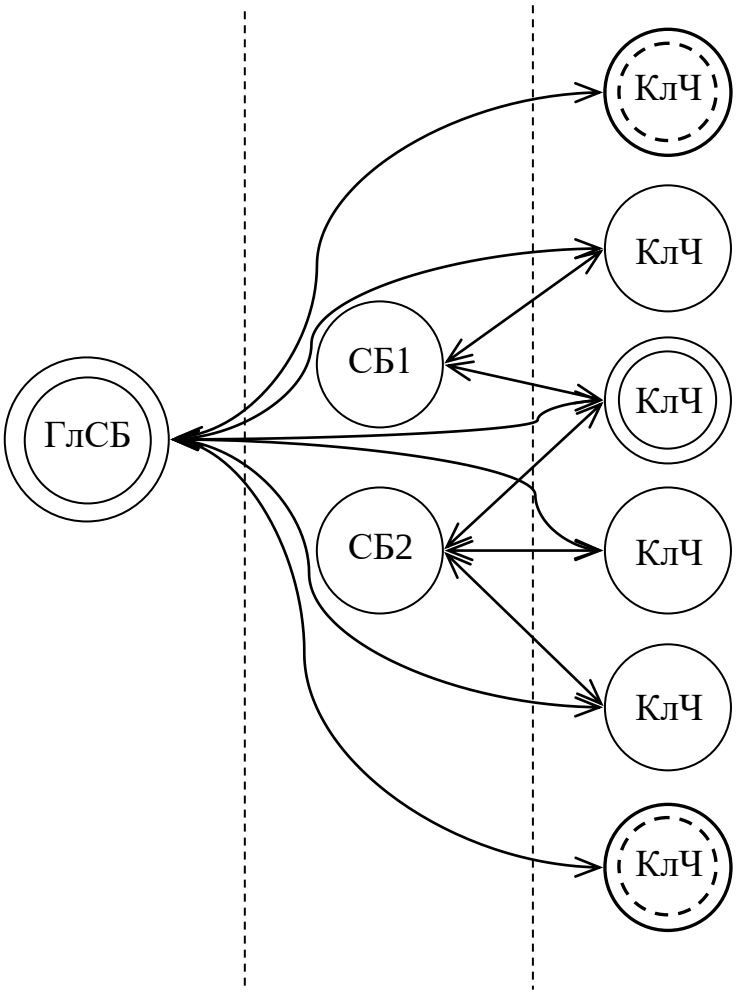

Рис. 7. Модель иерархического администрирования

В данной модели администрирования **на всех серверах низшего уровня иерархии** необходимо добавить автоматическое действие «Получить все настройки» в качестве реакции на события изменения настроек с сервера (серверов) безопасности высшего уровня иерархии, которых также может быть несколько.

При реализации моделей иерархического администрирования, подразумевающих наличие в сетевой системе защиты нескольких уровней иерархии серверов безопасности СЗИ ViPNet SafePoint, возможны следующие **регламенты администрирования и синхронизации настроек**, задаваемые **автоматическими действиям и на сервере безопасности высшего уровня иерархии**:

1. **Режим «взаимного доверия»** администраторов серверов безопасности разных уровней иерархии. Назначается автоматическое действие «Получить все настройки» на события изменения настроек клиентских частей СЗИ ViPNet SafePoint серверами безопасности более низкого уровня. В данном случае при внесении изменений в настройки клиентской части администраторами серверов безопасности любого уровня иерархии, будет происходить автоматическая синхронизация настроек, т.е. на всех серверах безопасности автоматически будут приниматься измененные настройки клиентской части.

2. **Режим «недоверия»** администраторов серверов безопасности разных уровней иерархии. Назначается автоматическое действие «Отправить все настройки» на события изменения настроек клиентских частей СЗИ ViPNet SafePoint серверами безопасности более низкого уровня. В этом случае редактирование настроек клиентских частей СЗИ ViPNet SafePoint будет доступно только администраторам серверов безопасности высшего уровня иерархии. Измененные настройки клиентских частей автоматически принимаются всеми серверами безопасности более низкого уровня иерархии.
3. **Режим «контроля»** администратором серверов безопасности высшего уровня иерархии действий администраторов серверов безопасности более низкого уровня иерархии. Автоматические действия не задаются – в данном случае, при изменении настроек клиентской части сервером безопасности более низкого уровня иерархии, на главном сервере будет появляться окно «Файлы настроек клиента – Ошибка проверки целостности настроек клиента», с отображением измененных файлов настроек. В данном окне администратор, проанализировав внесенные изменения, может выбрать соответствующий вариант действий:
   - Получить настройки с клиента;
   - Отправить настройки клиенту;
   - Игнорировать.

   Эти действия описаны выше.
4. **Режим «сохранения текущих настроек»** на сервере безопасности высшего уровня иерархии. В данном случае задается автоматическое действие «Игнорировать». При изменении настроек клиентской части СЗИ ViPNet SafePoint, на сервере безопасности высшего уровня иерархии останутся настройки, которые впоследствии могут быть отправлены (восстановлены с сервера) на клиентскую часть. При этом до восстановления настроек, на клиентской части будут действовать настройки, измененные сервером безопасности более низкого уровня иерархии серверов безопасности.

3. Реализация моделей администрирования и синхронизации настроек

3.1. Локальное администрирование. Клиентская часть СЗИ ViPNet SafePoint устанавливается на автономный компьютер или на компьютер в составе одноранговой сети

Данная конфигурация подразумевает установку только клиентской части СЗИ ViPNet SafePoint, при установке выбирается способ установки «Обычная». Процесс установки клиентской части СЗИ ViPNet SafePoint описан в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию».

Настройка всех механизмов контроля и разграничения прав доступа осуществляется при помощи интерфейса клиентской части СЗИ ViPNet SafePoint и описана в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию».

3.2. Локальное администрирование. Клиентская часть устанавливается на компьютер, входящий в состав доменной сети

Данная конфигурация подразумевает установку только клиентской части СЗИ ViPNet SafePoint, при установке выбирается способ установки «Обычная». Процесс установки клиентской части СЗИ ViPNet SafePoint описан в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию».

До перезагрузки компьютера после установки клиентской части СЗИ ViPNet SafePoint необходимо установить 3-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\InfoTeCS\ViPNet SafePoint\Common\PackageConfig), т.е. добавить 8 к имеющемуся значению, данное действие необходимо для получения возможности создания/редактирования пользователей домена.

После перезагрузки компьютера и запуска интерфейса управления настройками СЗИ ViPNet SafePoint, во вкладке «Учетные записи», при нажатии правой кнопкой мыши по области отображения списка учетных записей, администратору безопасности, который должен иметь права администратора домена, будет предоставлено на выбор два варианта обновления списка пользователей и групп (см. рис. 8):

1. Обновить списки пользователей и групп домена AD.
2. Обновить списки локальных пользователей групп.

Запускать интерфейс управления настройками СЗИ ViPNet SafePoint для работы (создания и редактирования) с доменными пользователями необходимо от имени учетной записи администратора домена.

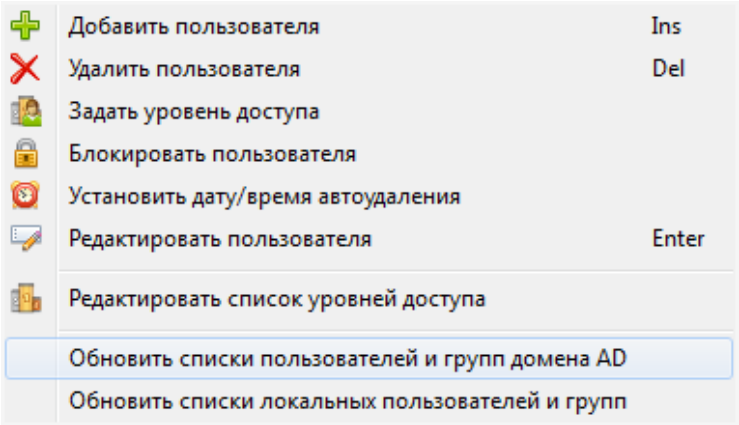

Рис. 8. Контекстное меню вкладки «Учетные записи»

После обновления списков пользователей и групп в интерфейсе управления настройками клиентской части СЗИ ViPNet SafePoint будут отображаться как доменные, так и локальные пользователи (см. рис. 9).

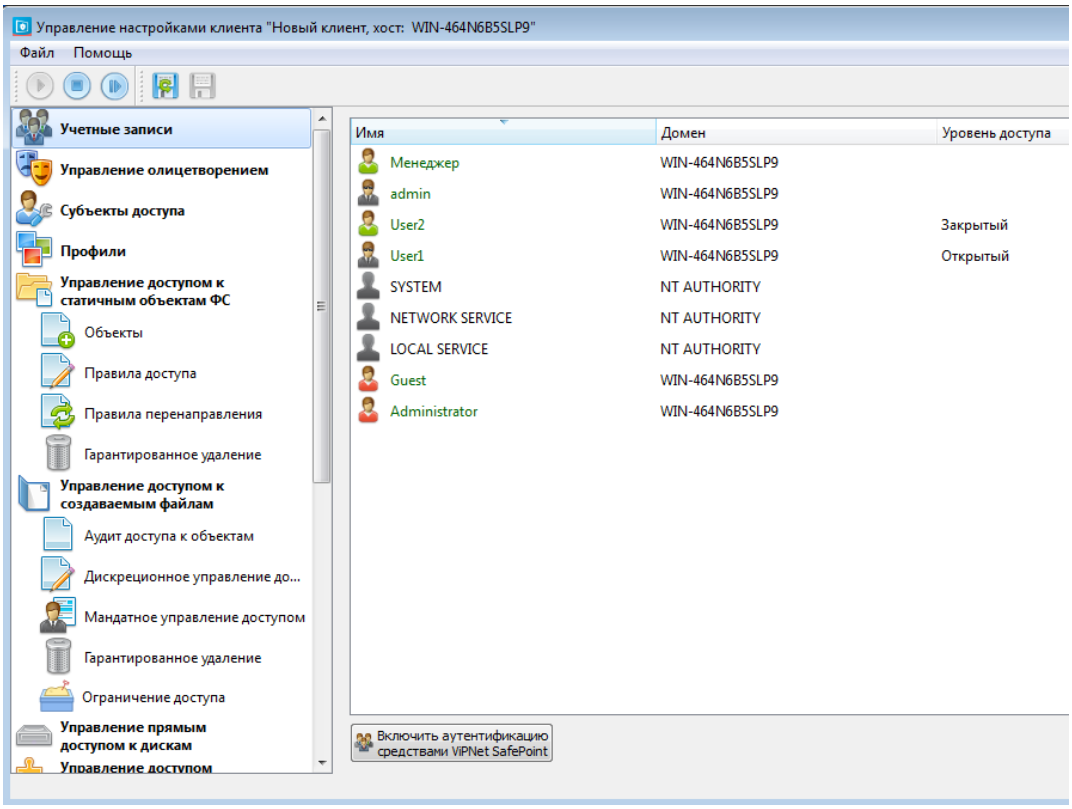

Рис. 9. Отображение пользователей в интерфейсе управления настройками

В интерфейсе для доменных пользователей в поле «Домен» указывается имя домена, для локальных пользователей – имя машины.

В данном случае пользователю (администратору безопасности) предоставляется возможность создания и редактирования, как доменных, так и локальных пользователей (см. рис. 10).

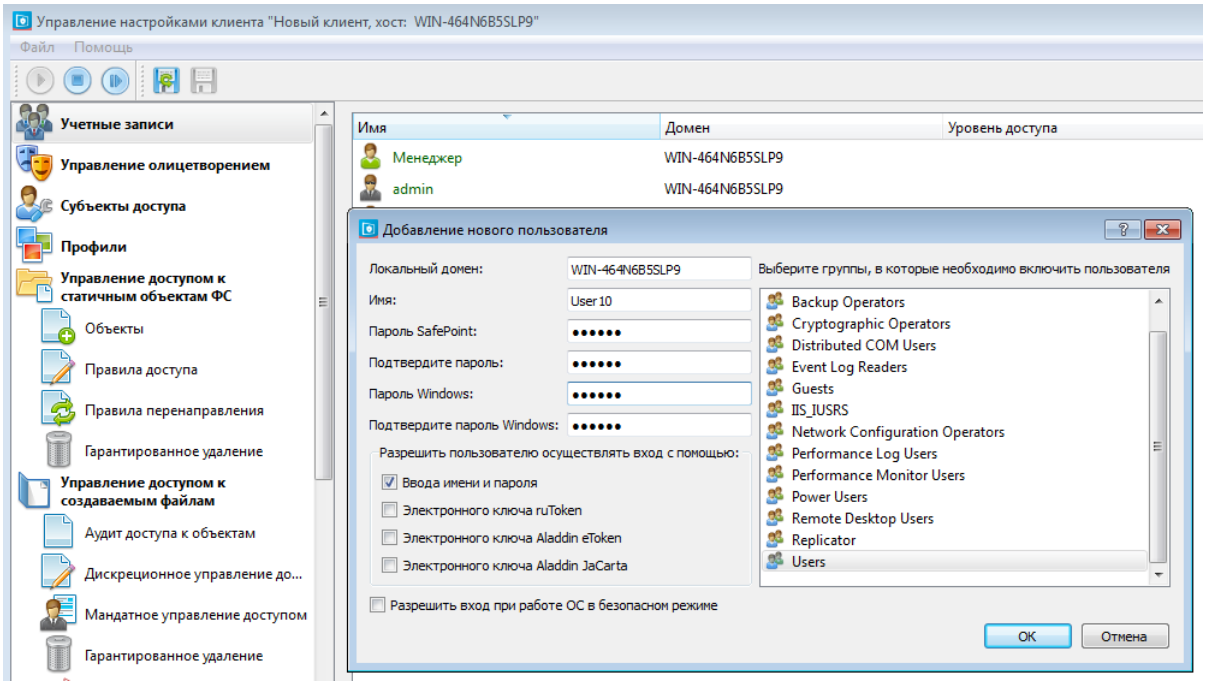

Рис. 10. Создание и редактирование пользователей

Дальнейшая настройка всех механизмов контроля и разграничения прав доступа описана в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию».

3.3. Сетевое неиерархическое администрирование с использование одного сервера безопасности СЗИ ViPNet SafePoint

3.3.1. Сервер безопасности и подключенные к нему клиентские части входят в состав одноранговой сети

При включении в схему администрирования сервера безопасности СЗИ ViPNet SafePoint настройка в любой момент времени может производиться с использованием только одного интерфейса управления настройками, либо локального (на клиентской части), либо с сервера безопасности (удаленно).

Данная конфигурация подразумевает установку клиентских частей СЗИ ViPNet SafePoint на защищаемые компьютеры, входящие в состав одноранговой сети, и установку на одном из компьютеров сервера безопасности СЗИ ViPNet SafePoint. Процесс установки клиентской части СЗИ ViPNet SafePoint описан в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию», процесс установки сервера безопасности СЗИ ViPNet SafePoint описан в документе «ViPNet SafePoint. Руководство администратора по удаленному администрированию».

Для реализации данной конфигурации в интерфейсе управления настройками клиентских частей СЗИ ViPNet SafePoint во вкладке «Настройки сети» необходимо прописать имя или IP адрес компьютера, с установленным сервером безопасности СЗИ ViPNet SafePoint, для подключения их к серверу безопасности СЗИ ViPNet SafePoint. Подробное описание данных действий приведено в документе «ViPNet SafePoint. Руководство администратора по локальному администрированию» (раздел «Первичная настройка. Запуск и остановка СЗИ ViPNet SafePoint»).

Работа с сервером безопасности СЗИ ViPNet SafePoint описана в документе «ViPNet SafePoint. Руководство администратора по удаленному администрированию», в данном документе приводятся примеры использования компонентов СЗИ ViPNet SafePoint в различных конфигурациях.

При администрировании (удаленной настройке) клиентских частей СЗИ ViPNet SafePoint в данном случае возможны следующие варианты:

1. Администратор безопасности проводит всю **настройку** (кроме первичной – подключение клиентских частей к серверу безопасности) клиентских частей СЗИ ViPNet SafePoint с выделенного места – компьютера с установленным **сервером безопасности** СЗИ ViPNet SafePoint. В данном случае в качестве общих автоматических действий на сервере безопасности СЗИ ViPNet SafePoint для синхронизации настроек следует задать «Отправить все настройки» (см. рис. 11).

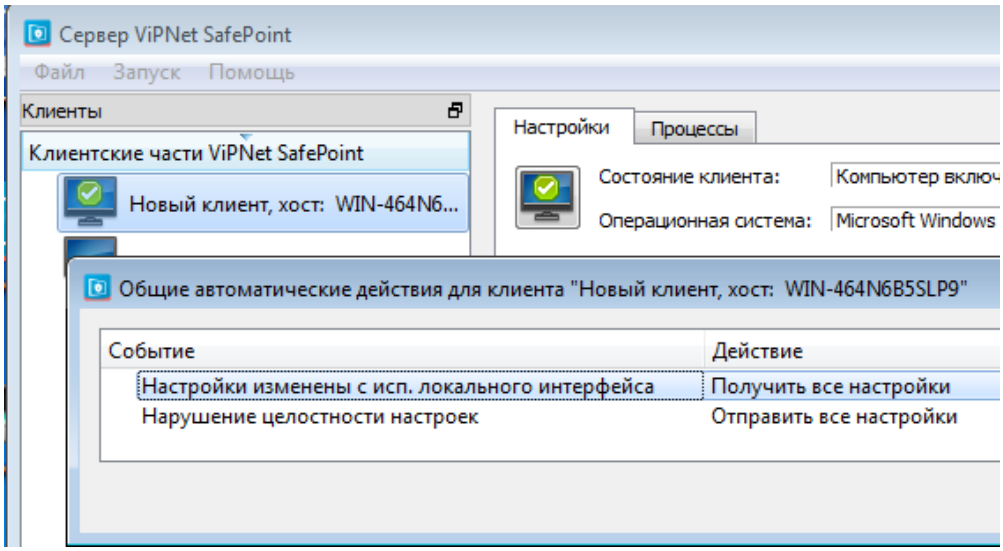

Рис. 11. Назначенные общие автоматические действия

В журнале событий на сервере безопасности фиксируются события, связанные с изменением настроек механизмов защиты на клиентских машинах и соответствующую реакцию со стороны сервера безопасности на эти события, также в журнале фиксируются действия администратора безопасности по получению или передаче настроек с сервера безопасности СЗИ ViPNet SafePoint. Журнал представлен на рис. 12.

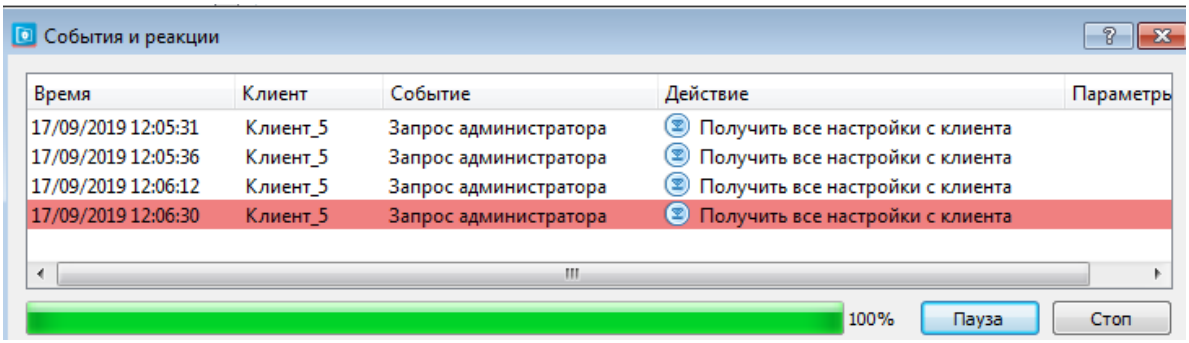

Рис. 12. Журнал «Событий и реакций»

2. **Настройка** производится как **локально**, так и с компьютера с установленным **сервером безопасности** СЗИ ViPNet SafePoint. В данном случае на сервере следует задать автоматические действия, представленные на рис. 13.

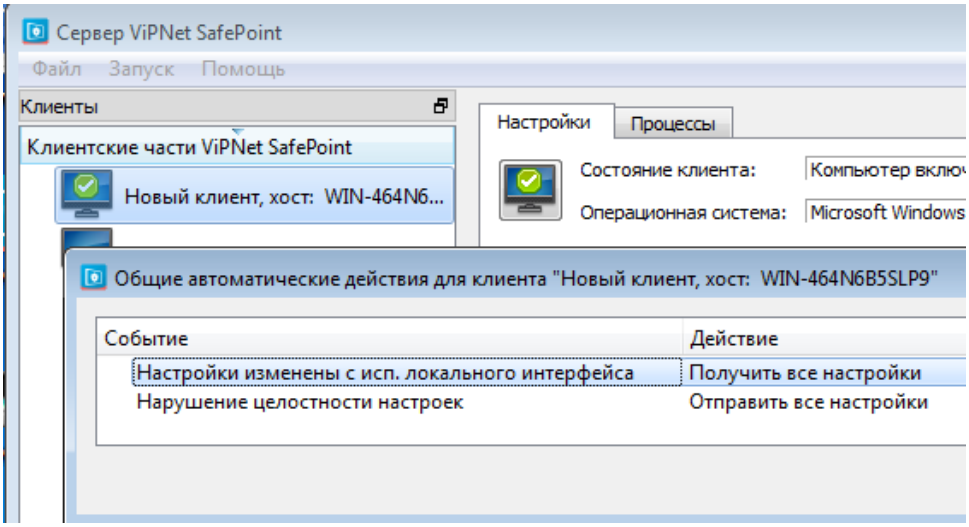

Рис. 13. Назначенные общие автоматические действия

Соответствующие события синхронизации настроек будут фиксироваться в журнале «Событий и реакций», см. рис. 14.

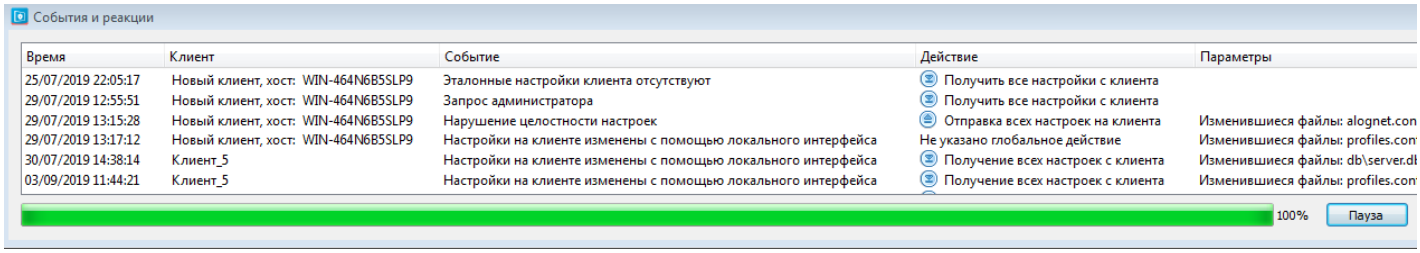

Рис. 14. Журнал «Событий и реакций»

Список общих автоматических действий может быть задан как для всех клиентских частей, подключенных к данному серверу безопасности, так и для каждой клиентской части в отдельности. Эта возможность позволяет администратору безопасности самостоятельно решать задачу регламентирования администрирования клиентских частей СЗИ ViPNet SafePoint.

3.3.2. Сервер безопасности и подключенные к нему клиентские части входят в состав доменной сети – назначение главного сервера безопасности

В данной конфигурации сервер безопасности СЗИ ViPNet SafePoint следует назначить главным по пользователям в домене следующим образом. При установке сервера безопасности СЗИ ViPNet SafePoint **до перезагрузки** компьютера необходимо установить 1-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config), т.е. добавить 2 к имеющемуся значению, процессустановки сервера безопасности СЗИ ViPNet SafePoint описан в документе «ViPNet SafePoint. Руководство администратора по удаленному администрированию».

После подключения всех клиентских частей к серверу безопасности СЗИ ViPNet SafePoint при необходимости изменения (редактирования) базы данных доменных пользователей на компьютере, с установленным сервером безопасности (это может быть, как компьютер, являющийся сервером домена, так и любой иной компьютер, входящий в данный домен), необходимо запустить специальную утилиту – утилита управления доменными пользователями (см. рис. 15).

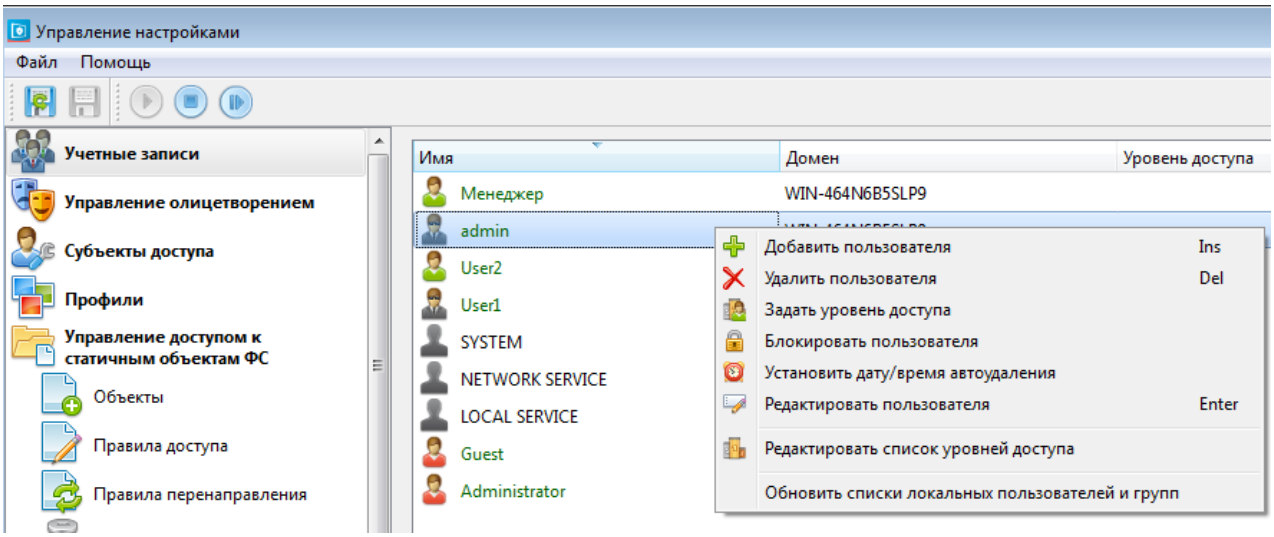

Рис. 15. Интерфейс утилиты управления доменными пользователями

Работа с утилитой управления доменными пользователями и сервером безопасности СЗИ ViPNet SafePoint описана в документе «ViPNet SafePoint. Руководство администратора по удаленному администрированию».

После внесения изменений в базу данных доменных пользователей, обновленная база будет разослана на все клиентские части, подключенные к данному серверу безопасности СЗИ ViPNet SafePoint. Остальные действия, относящиеся к процессу администрирования (настройки) клиентских частей СЗИ ViPNet SafePoint аналогичны процессу администрирования в одноранговой сети.

3.4. Сетевое неиерархическое администрирование с использование нескольких серверов безопасности СЗИ ViPNet SafePoint

3.4.1. Полное резервирование серверов безопасности

В данном случае резервирование подразумевает наличие двух (или более) равнозначных серверов безопасности СЗИ ViPNet SafePoint, имеющих одинаковые возможности по администрированию клиентских частей СЗИ ViPNet SafePoint.

Общие автоматические действия при этом могут быть настроены исходя из вариантов администрирования, рассмотренных в разделе 2.4.1, также необходимо определить регламент работы (договоренность) администраторов серверов безопасности СЗИ ViPNet SafePoint.

Только один из серверов безопасности должен назначаться главным по пользователям домена (установлен 1-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config)).

3.4.1.1. Режим «взаимного доверия»

Настройка клиентских частей СЗИ ViPNet SafePoint происходит **только с серверов безопасности**.

На серверах безопасности СЗИ ViPNet SafePoint задан следующий регламент работы между серверами безопасности:

- автоматические действия для подключенных клиентских частей, заданы таким образом, что если настройки изменены с одного из серверов безопасности, то другой их (измененные файлы настроек) автоматически принимает (см. рис. 16).

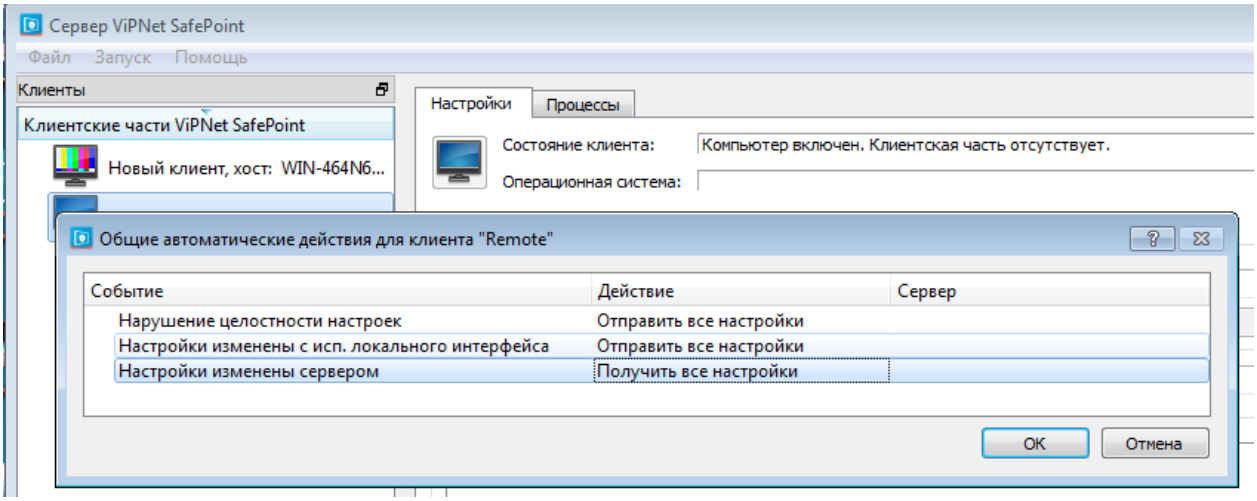

Рис. 16. Назначенные общие автоматические действия

В данном случае администраторы безопасности «доверяют» друг другу и автоматически происходит синхронизация настроек.

Журнал «Событий и реакций», формируемый на серверах безопасности представлен на рис. 17.

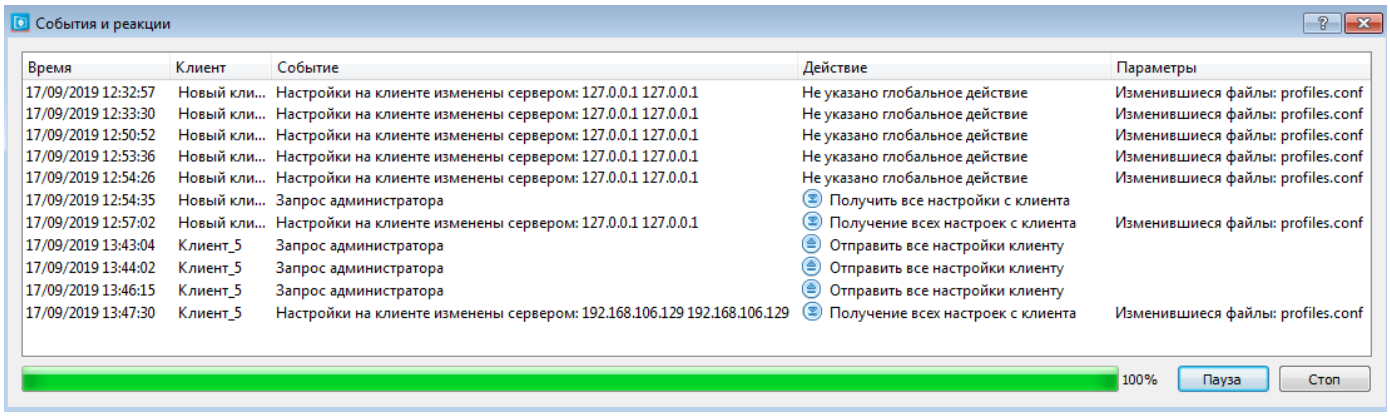

Рис. 17. Журнал «Событий и реакций»

Настройка клиентских частей СЗИ ViPNet SafePoint происходит, **как с серверов безопасности**, **так и локально** – из интерфейса клиентской части.

На серверах безопасности СЗИ ViPNet SafePoint задан следующий регламент работы между серверами безопасности:

- автоматические действия заданы таким образом, что если настройки клиентской части изменены с одного из серверов безопасности, то другие серверы безопасности их автоматически принимают, если настройки изменены локально, то серверы безопасности автоматически принимают измененные настройки (см. рис. 18).

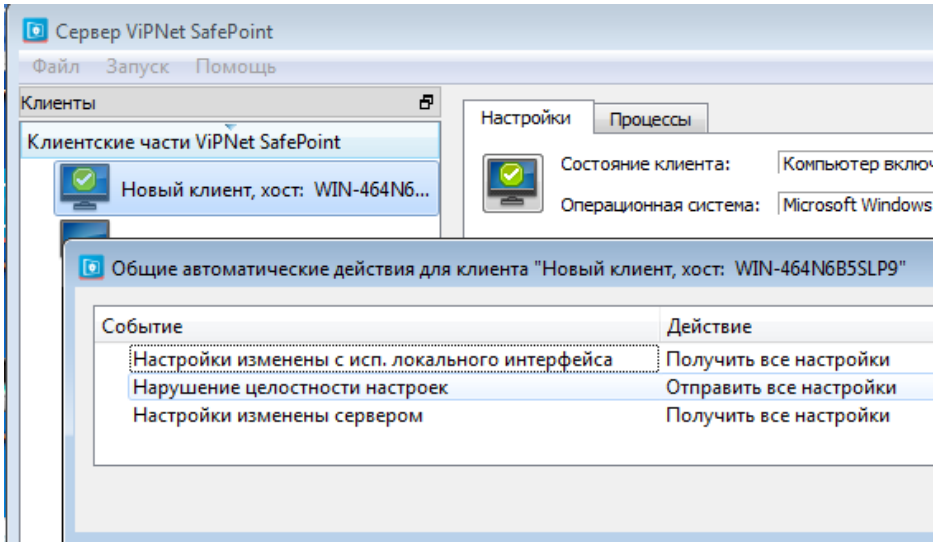

Рис. 18. Назначенные общие автоматические действия

При данной конфигурации журнал «Событий и реакций» имеет вид, представленный на рис. 19.

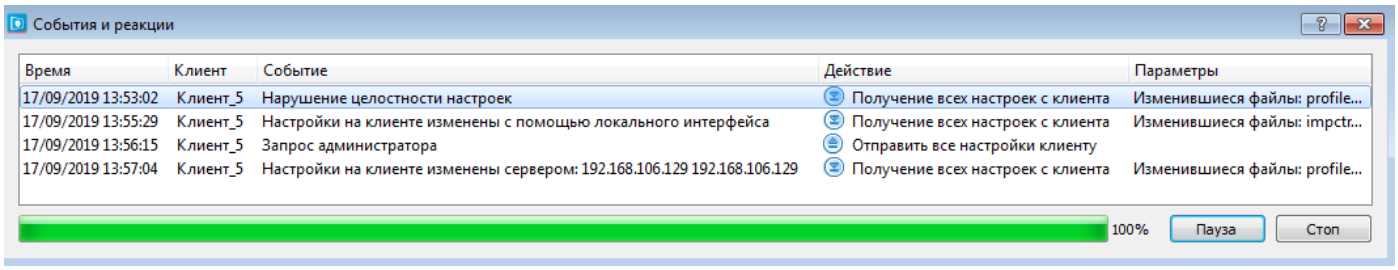

Рис. 19. Журнал «Событий и реакций»

3.4.1.2. Режим «недоверия»

Настройка клиентских частей СЗИ «ViPNet SafePoint» происходит **только с серверов безопасности**.

На серверах безопасности СЗИ ViPNet SafePoint не задается регламент работы между серверами безопасности (не настроены автоматические действия) (см. рис. 20).

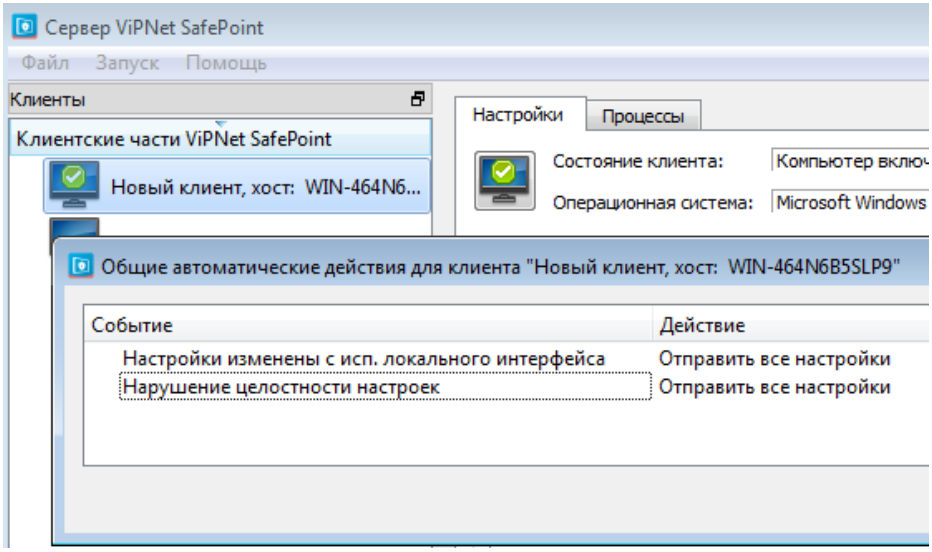

Рис. 20. Назначенные общие автоматические действия

В данном случае, при изменении настроек клиентской части с одного сервера безопасности на другом (других) появится окно «Файлы настроек клиента «Имя_клиента»» с указанием какой файл (какие файлы) были изменены (см. рис. 21).

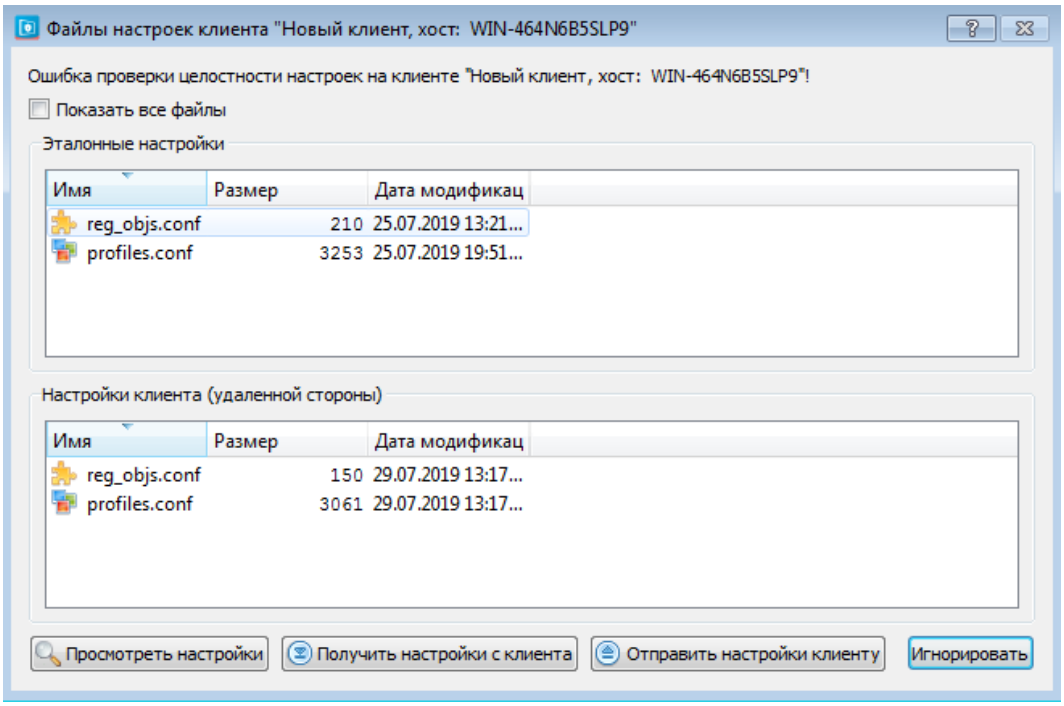

Рис. 21. Окно «Файлы настроек клиента»

В данном окне администратор безопасности может выбрать одно из предложенных действий:

1) Отправить настройки. В данном случае на клиентскую часть будут отправлены настройки, хранящиеся на сервере, после чего на первом сервере безопасности появится аналогичное окно «Файлы настроек клиента «Имя_клиента»» с указанием какой файл (какие файлы) были изменены.

В данном случае администраторы серверов безопасности должны прийти к соглашению о том, какие настройки должны вступить в силу.

2) Принять настройки. Выбор данного действия означает, что администратор безопасности согласен с изменениями, внесенными другим администратором сервера безопасности, файлы настроек, хранящиеся на сервере безопасности, будут изменены.
3) Игнорировать. Выбрав данное действие, при следующем подключении клиентской части к серверу безопасности вновь появится окно «Файлы настроек клиента «Имя_клиента»» с указанием того, какой файл (какие файлы) были изменены.

При данной конфигурации журнал «Событий и реакций» будет иметь вид, представленный на рис. 22.

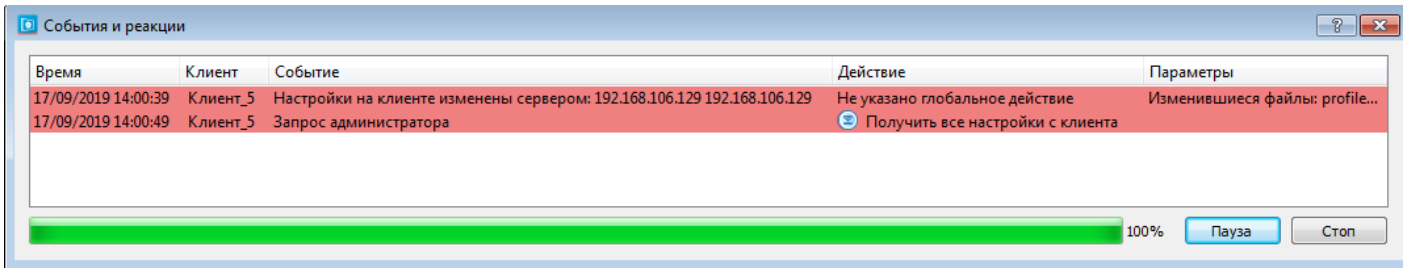

Рис. 22. Журнал «Событий и реакций»

Настройка клиентских частей СЗИ ViPNet SafePoint происходит **как с серверов безопасности, так и локально** из интерфейса клиентской части.

На серверах безопасности СЗИ ViPNet SafePoint не задается регламент работы между серверами безопасности (не настроены автоматические действия) (см. рис. 23).

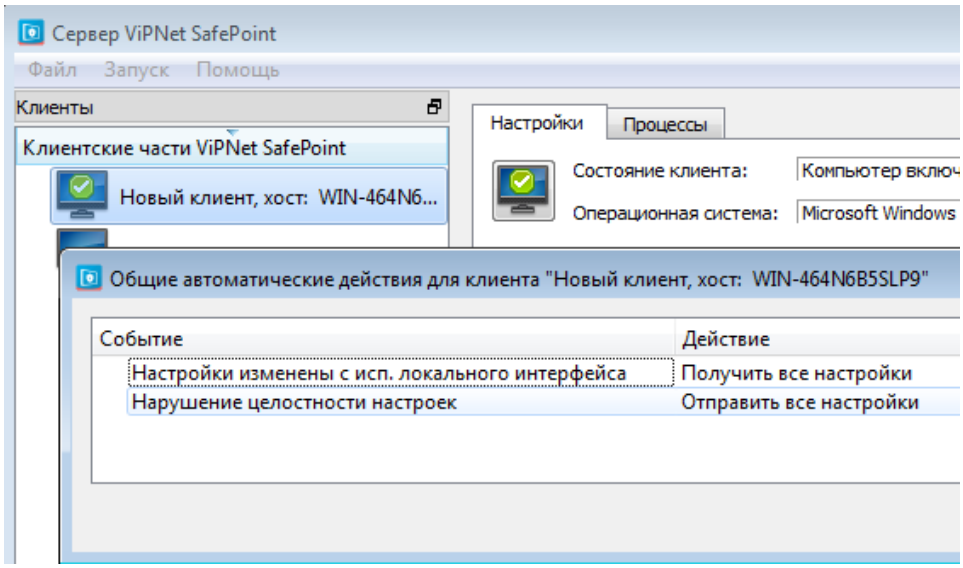

Рис. 23. Назначенные общие автоматические действия

При данной конфигурации при изменении настроек клиентской части с одного сервера безопасности на другом (других) появится окно «Файлы настроек клиента «Имя_клиента»» с указанием какой файл (какие файлы) были изменены (см. рис. 21). В данном окне администратор безопасности может выбрать одно из предложенных действий:

1) Отправить настройки. В данном случае на клиентскую часть будут отправлены настройки, хранящиеся на сервере, после чего на первом сервере безопасности появится аналогичное окно «Файлы настроек клиента «Имя_клиента»» с указанием какой файл (какие файлы) были изменены.

В данном случае администраторы серверов безопасности должны прийти к соглашению о том, какие настройки должны вступить в силу.

2) Принять настройки. Выбор данного действия означает, что администратор безопасности согласен с изменениями, внесенными другим администратором

сервера безопасности, файлы настроек, хранящиеся на сервере безопасности, будут изменены.

3) Игнорировать. Выбрав данное действие, при следующем подключении клиентской части к серверу безопасности вновь появится окно «Файлы настроек клиента «Имя_клиента»» с указанием какой файл (какие файлы) были изменены.

При данной конфигурации журнал «Событий и реакций» будет иметь вид, представленный на рис. 24.

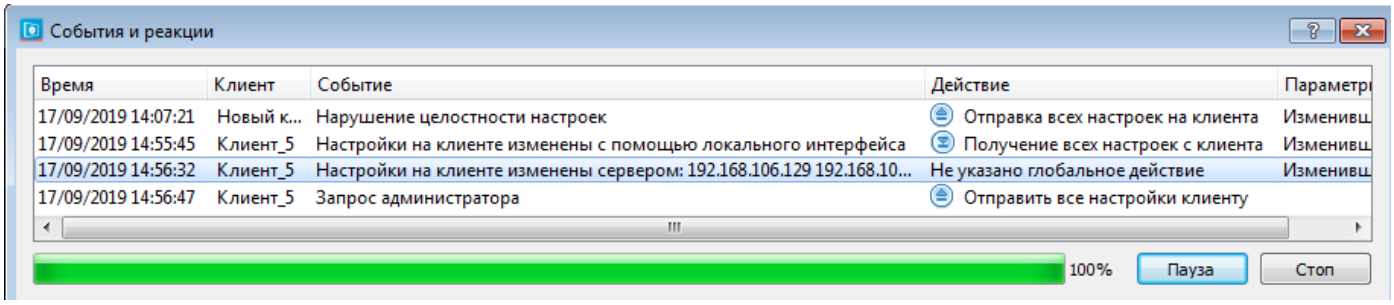

Рис. 24. Журнал «Событий и реакций»

3.4.1.3. Особенности реализации в доменной сети

При реализации полного резервирования серверов безопасности в доменной сети, отличие от полного резервирования в одноранговой сети состоит в том, что необходимо установить регламент изменения списка (базы данных) доменных пользователей. Возможно два варианта задания **базы данных доменных пользователей**:

1. **Без задания автоматических действий.** При этом при изменении базы данных пользователей домена на сервера безопасности будет приходить оповещение (окно «Файлы настроек клиента»), в котором администратору будет предоставлен выбор получить настройки, отправить настройки или игнорировать (для каждого клиента, подключенного к серверу безопасности, будет появляться свое окно), в данном варианте администраторам необходимо договориться (см. рис. 21).

Журнал «Событий и реакций» будет иметь следующий вид (см. рис. 25).

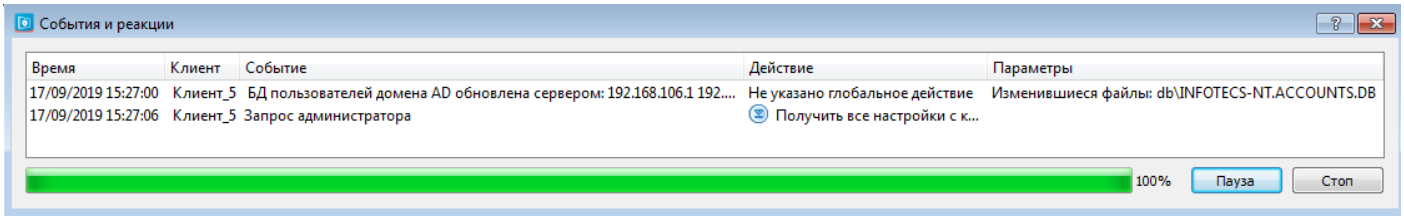

Рис. 25. Журнал «Событий и реакций»

2. **С заданием автоматических действий.** На серверах безопасности СЗИ ViPNet SafePoint задан следующий регламент работы между серверами безопасности:

- автоматические действие для подключенных клиентских частей, заданы таким образом, что если обновлена база данных (БД) пользователей домена ADодним сервером безопасности, то другой её (измененную БД пользователей домена AD) автоматически принимает (см. рис. 26).

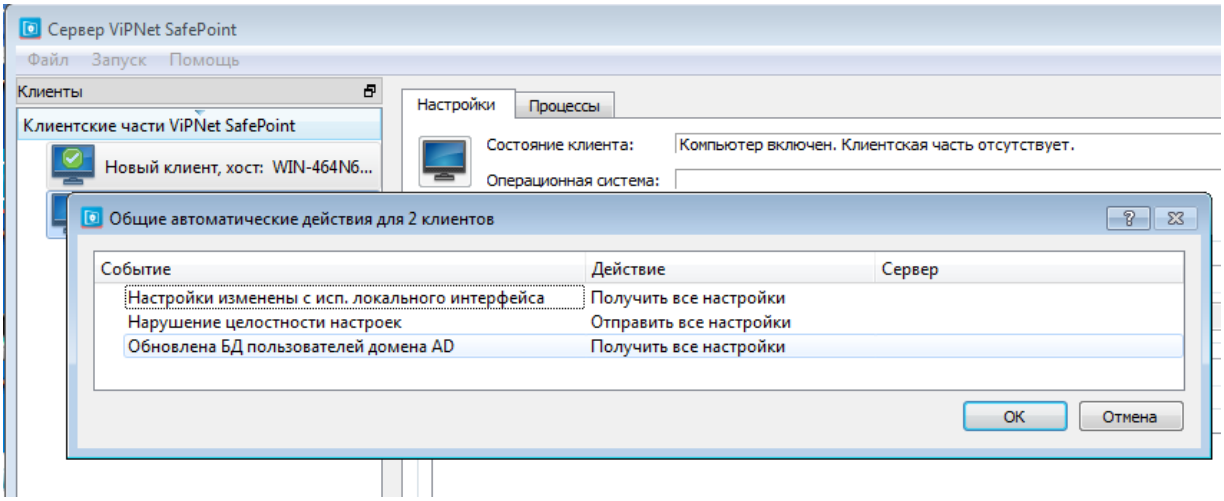

Рис. 26. Назначенные общие автоматические действия

Журнал «События и реакции» в данном случае при изменении базы данных доменных пользователей будет иметь вид, представленный на рис.27.

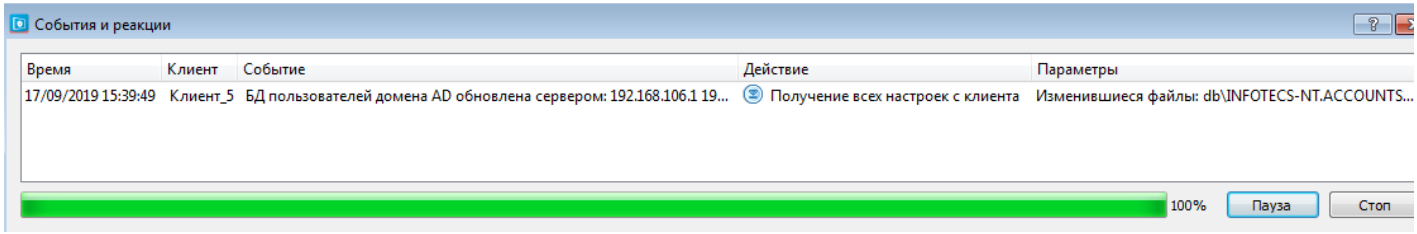

Рис. 27. Журнал «Событий и реакций»

3.4.2. Резервирование серверов безопасности при наличии критичных объектов защиты

В данном случае резервирование подразумевает наличие двух (или более) серверов безопасности СЗИ ViPNet SafePoint.

Для критически важных объектов общие автоматические действия следует назначать согласно разделу 3.3 «Сетевое неиерархическое администрирование с использование одного сервера безопасности СЗИ ViPNet SafePoint».

Для остальных клиентских частей общие автоматические действия следует назначать согласно разделу 3.4.1 «Полное резервирование серверов безопасности».

3.4.3. Разделение нагрузки и выделение критичных объектов защиты)

В данном случае резервирование подразумевает наличие двух (или более) серверов безопасности СЗИ ViPNet SafePoint.

Для удобства администрирования администратор безопасности на сервере безопасности может сформировать логическую структуру подключенных клиентских частей СЗИ ViPNet SafePoint (см. рис. 28).

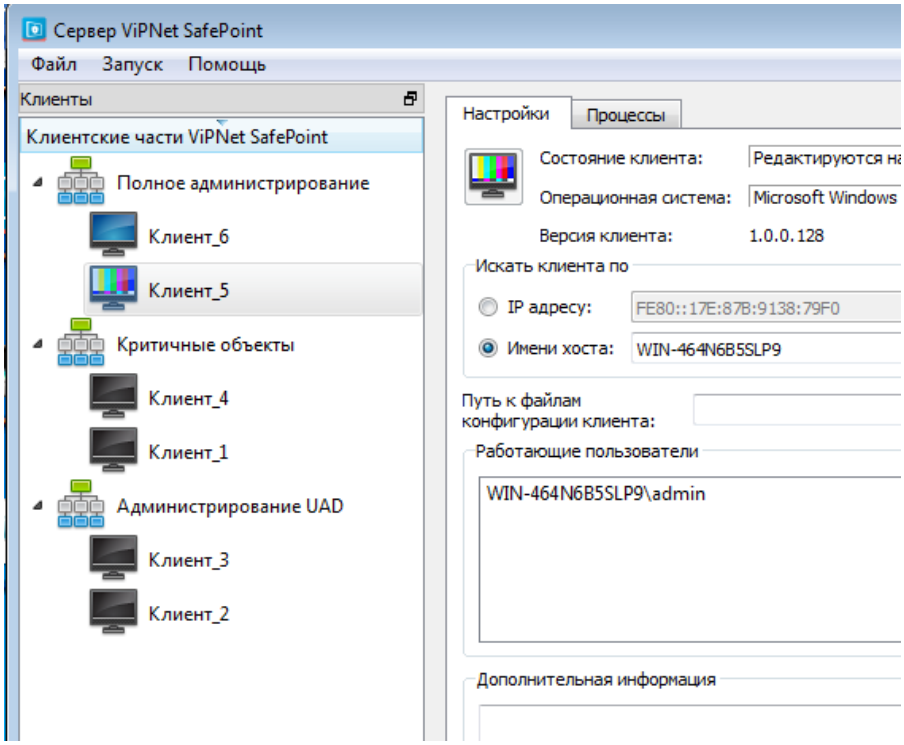

Рис. 28. Логическое разделение подключенных клиентских частей

На сервере безопасности, к которому подключены все клиентские части **для** тех **не критически важных клиентских частей** СЗИ ViPNet SafePoint, которые *подключены только к нему* общие автоматические действия следует назначать согласно разделу 3.3. «Сетевое неиерархическое администрирование с использование одного сервера безопасности СЗИ ViPNet SafePoint». На сервере безопасности, к которому подключены все клиентские части **для** тех **не критически важных клиентских частей** СЗИ ViPNet SafePoint, которые *подключены ещё к какому-либо другому* серверу безопасности следует добавить автоматические действия:

- реакцию «Отправить все настройки» на событие «Обновлена база данных пользователей домена AD»;
- реакцию «Получить все настройки» на событие «Настройки изменены сервером» (с указанием IP адреса или имени другого сервера безопасности);

На других серверах безопасности следует добавить автоматические действия:

- реакцию «Получить все настройки» на событие «Обновлена база данных пользователей домена AD» (с указанием IP адреса или имени сервера безопасности, с которого осуществляется администрирование базы данных пользователей домена);
- для некритичных клиентских частей, которые подключены только к данному серверу безопасности (помимо сервера безопасности, с которого осуществляется администрирование базы данных пользователей домена) общие автоматические действия следует назначать согласно разделу 3.3. «Сетевое неиерархическое администрирование с использование одного сервера безопасности СЗИ ViPNet SafePoint».

Для не критически важных клиентских частей СЗИ ViPNet SafePoint настройка общих автоматических действий для данной конфигурации описана в разделе 3.3.1.

3.5. Сетевое иерархическое администрирование

Модели администрирования, описанные ранее в документе, могут быть применены как для серверов безопасности низшего уровня иерархии серверов безопасности, так и для серверов безопасности более высокого уровня иерархии серверов безопасности СЗИ ViPNet SafePoint.

При реализации сетевого иерархического администрирования **в доменной сети** следует назначить главным по пользователям домена только один из серверов безопасности (установлен 1-й бит в значении параметра «Package Config» (HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config)). При этом все клиентские части должны быть подключены к данному серверу безопасности.

3.5.1. Сетевое иерархическое администрирование с одним сервером безопасности высшего уровня иерархии (главный сервер безопасности)

Для реализации модели администрирования с одним главным сервером безопасности (сервер безопасности высшего уровня иерархии) все клиентские части должны быть подключены к данному серверу безопасности.

В данной модели администрирования **на всех серверах низшего уровня иерархии** необходимо добавить автоматическое действие «Получить все настройки» в качестве реакции на событие «Настройки изменены сервером» (с указанием IP адреса или имени главного сервера безопасности), остальные автоматические действия серверов безопасности низшего уровня иерархии могут быть настроены исходя из вариантов, рассмотренных в разделе 2.4.

В журнале «События и реакции» на главном сервере безопасности будут отображаться соответствующие записи о произошедших изменениях настроек клиентских частей СЗИ ViPNet SafePoint.

При наличии критически важных защищаемых объектов, администрирование которых может быть доверено только администратору безопасности главного сервера безопасности, общие автоматические действия следует назначить исходя из вариантов, рассмотренных в разделе 3.3«Сетевое неиерархическое администрирование с использование одного сервера безопасности СЗИ ViPNet SafePoint».

3.5.2. Сетевое иерархическое администрирование с несколькими серверами безопасности высшего уровня иерархии

В данном случае предполагается наличие двух и более серверов безопасности высшего уровня иерархии серверов безопасности СЗИ ViPNet SafePoint.

При данной конфигурации средствами СЗИ ViPNet SafePoint может быть реализовано:

- полное резервирование серверов безопасности – все клиентские части СЗИ ViPNet SafePoint подключаются ко всем серверам безопасности СЗИ ViPNet SafePoint высшего уровня иерархии;
- выделение критически важных защищаемых объектов –выделенные клиентские части подключаются к одному из серверов безопасности высшего уровня иерархии;
- разделение нагрузки между серверами безопасности высшего уровня иерархии и/или реализация полного резервирования серверов безопасности для критически важных защищаемых объектов.

Общие автоматические действия при этом могут быть настроены исходя из вариантов администрирования, описанных в разделе 3.4, дополнительно необходимо определить регламент работы администраторов серверов безопасности СЗИ ViPNet SafePoint высшего уровня иерархии (режимы «доверия» и «недоверия»).

4. Использование серверов аудита

Сервер аудита СЗИ ViPNet SafePoint является отдельным самостоятельным компонентом в части ведения и анализа аудита, поэтому сервер (серверы) аудита может быть установлен на выделенном компьютере или совмещен с другими компонентами СЗИ ViPNet SafePoint, в частности с сервером безопасности.

Сервер аудита служит как для получения сообщений о событиях безопасности на удаленных защищаемых компьютерах, как в отношении критичных событий в режиме реального времени (при запущенном интерфейсе сервера аудита), так и применительно к остальным контролируемым событиям безопасности по запросу администратора, т.е. в режиме интерактивного аудита. Работа с сервером аудита описана в документе «ViPNet SafePoint. Руководство администратора по удаленному администрированию».

Число серверов аудита, к которым может быть подключена любая клиентская часть СЗИ ViPNet SafePoint, не ограничено. Это обусловливает возможность одновременного использования в сети нескольких серверов аудита, по аналогии с серверами безопасности (только без иерархии), как с целью их полного, так и частичного резервирования, в том числе, и для реализации на отдельном сервере аудита событий безопасности, происходящих на критически важных, с точки зрения обрабатываемой информации, объектах защиты.

С учетом того, что сервер безопасности и сервер аудита независимые компоненты сетевой системы защиты, может формироваться выделенное рабочее место (сервер) аудита событий безопасности.

Иерархическая структура для серверов аудита не предусмотрена.

5. Усечение возможностей серверов безопасности и аудита для администрирования критически важных объектов

В общем случае, как с сервера безопасности, так и с сервера аудита, администратор может воспользоваться возможностью завершения процесса, обзора файловой системы и реестра удаленной клиентской машины.

Возможности завершения процесса и обзоров файловой системы и реестра доступны с сервера аудита только, если сервер аудита установлен на одной машине с сервером безопасности и интерфейс сервера безопасности активен.

При наличии в составе защищаемых объектов критически важного объекта, для него данные возможности могут быть отключены. Для отключения возможности завершения процесса и обзора файловой системы и реестра, при установке клиентской части СЗИ ViPNet SafePoint необходимо добавить 16 к имеющемуся значению параметра HKEY_LOCAL_MACHINE\SOFTWARE\INFOTECS\VIPNET SAFEPOINT\Common\Package Config (установить 4-й бит).

С целью полного ограничения возможности доступа администратора безопасности к информации, обрабатываемой на критически важном защищаемом объекте, клиентская часть, устанавливаемая на данный компьютер, не должна соединяться с серверами безопасности – настройка должна осуществляться из локального интерфейса под соответствующим надзором за действиями администратора.

С целью же возможности оперативного контроля происходящих на таком компьютере событий безопасности, установленная на нем клиентская часть СЗИ ViPNet SafePoint должна подключаться к серверу аудита, для которого в отношении данной клиентской части будет исключена возможность завершения процесса, обзора файловой системы и реестра удаленной клиентской машины.

Список сокращений

AD	active directory
АРМ	автоматизированное рабочее место
БД	база данных
СЗИ	система защиты информации
ОС	операционная система